HD

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/694,000	10/28/2003	E. DeVere Henderson	117474	3673

25944 7590 01/28/2008

OLIFF & BERRIDGE, PLC
P.O. BOX 320850
ALEXANDRIA, VA 22320-4850

EXAMINER	
RAPILLO, KRISTINE K	
ART UNIT	**PAPER NUMBER**
3626	

MAIL DATE	DELIVERY MODE
01/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/694,000	HENDERSON, E. DEVERE	
	Examiner	Art Unit	
	KRISTINE K. RAPILLO	3626	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/ are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1 – 27 are pending.

Specification

1. The disclosure is objected to because of the following informalities:

Typographical errors.

The reference character for the probability of attack node (corresponding to Figure 2) is 110; however, paragraph [0049] of the specification documents the probability of attack node as 10.

The reference character for the risk level portion (corresponding to Figure 3) is 221; however, paragraph [0058] of the specification documents the risk level portion as 201.

Appropriate correction is required.

Double Patenting

1. Claims 1 – 3, 6 – 12, 15 – 21, and 24 - 27 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 - 21 of copending Application No. 10/694,081 (Henderson et al.). Although the conflicting claims are not identical, they are not patentably distinct from each other because all the limitations of U.S. Application No. 10/694,000 are covered in the claims of U.S. Application No. 10/694,081.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

2. The table below is a comparison of all obvious type double patenting claims. The differences between the claims have been bolded and a summary of the rejection is included directly below the affected claims.

Application 10/694,000		Reference Application: 10/694,081
1. A method for **assessing risks of** a property due to terrorist activities, comprising: providing expert data, the expert data containing information regarding a possible attack from a terrorist group on the property; determining a plurality of variables based on the provided expert data, each variable characterizes an aspect of one of the possible attack and the property; formulating a hierarchy in which the plurality of variables are interconnected based on the provided expert data; determining a state for each of the plurality of variables based on the formulated hierarchy and the provided expert data; generating a model regarding the possible attack based on the determined states of the plurality of variables and the provided expert data; and Assessing risks of the property under the possible attack by the terrorist group based on the generated model.		1. A method for **establishing an insurance premium usable to insure against risk to** a property due to terrorist activities, comprising: providing expert data, the expert data containing information regarding a possible attack from a terrorist group on the property; determining a plurality of variables based on the provided expert data, each variable characterizes an aspect of one of the possible attack and the property; formulating a hierarchy in which the plurality of variables are interconnected based on the provided expert data; determining a state for each of the plurality of variables based on the formulated hierarchy and the provided expert data; generating a model regarding the possible attack based on the determined states of the plurality of variables and the provided expert data, assessing risks of the property under the possible attack by the terrorist group based on the generated model; and **establishing the insurance premium for the property based on the assessed risks.**
In regard to claim 1, the same function, risk assessment or analysis, is required to determine the risk to a property and to generate an insurance premium. The risk to a property is a component of determining an insurance premium. Therefore, claim 1 of this application is not patentably distinct from claim 1 of application 10/694,081.		
2. The method according to claim 1, wherein		2. The method according to claim 1, wherein

Application 10/694,000		Reference Application: 10/694,081
generating the model comprises: generating a hypothesis regarding the possible attack based on the formulated hierarchy and the provided expert data; initializing the model based on the generated hypothesis and the provided expert data; and updating the model based on information outside the generated hypothesis and the provided expert data.		generating the model comprises: generating a hypothesis regarding the possible attack based on the formulated hierarchy and the provided expert data; initializing the model based on the generated hypothesis and the provided expert data; and updating the model based on information outside the generated hypothesis and the provided expert data.
Claim 2 of this application is not patentably distinct from Claim 2 of application 10/694,081.		
3. The method according to claim 1, wherein determining a state for each of the plurality of variables comprises determining a linkage between a first variable and a second variable.		3. The method according to claim 1, wherein determining a state for each of the plurality of variables comprises determining a linkage between a first variable and a second variable.
Claim 3 of this application is not patentably distinct from Claim 3 of application 10/694,081.		
6. The method according to claim 1, wherein providing expert data comprises providing information regarding a goal of the terrorist group.		4. The method according to claim 1, wherein providing expert data comprises providing information regarding a goal of the terrorist group.
Claim 6 of this application is not patentably distinct from Claim 4 of application 10/694,081.		
7. The method according to claim 1, wherein providing expert data comprises providing information regarding an attack delivery method of the terrorist group.		5. The method according to claim 1, wherein providing expert data comprises providing information regarding an attack delivery method of the terrorist group.
Claim 7 of this application is not patentably distinct from Claim 5 of application 10/694,081.		
8. The method according to claim 1, wherein providing expert data comprises providing information regarding a weapon likely to be deployed by the terrorist group against the property.		6. The method according to claim 1, wherein providing expert data comprises providing information regarding a weapon likely to be deployed by the terrorist group against the property.
Claim 8 of this application is not patentably distinct from Claim 6 of application 10/694,081.		
9. The method according to claim 1, wherein providing expert data comprises providing information regarding a mode of the terrorist group to carry out the possible attack against the property.		7. The method according to claim 1, wherein providing expert data comprises providing information regarding a mode of the terrorist group to carry out the possible attack against the property.
Claim 9 of this application is not patentably distinct from Claim 7 of application 10/694,081.		

Application 10/694,000		Reference Application: 10/694,081
10. A computer storage medium having executable software code for **assessing risks of** a property due to terrorist activities, the executable software code including: instructions for providing expert data, the expert data containing information regarding a possible attack from a terrorist group on the property; instructions for determining a plurality of variables based on the provided expert data, each variable characterizes an aspect of one of the possible attack and the property; instructions for formulating a hierarchy in which the plurality of variables are interconnected based on the provided expert data; instructions for determining a state for each of the plurality of variables based on the formulated hierarchy and the provided expert data; instructions for generating a model regarding the possible attack based on the determined states of the plurality of variables and the provided expert data; and instructions for assessing risks of the property under the possible attack by the terrorist group based on the generated model.		8. A computer storage medium having executable software code for **establishing an insurance premium usable to insure against risk to** a property due to terrorist activities, the executable software code including: instructions for providing expert data, the expert data containing information regarding a possible attack from a terrorist group on the property; instructions for determining a plurality of variables based on the provided expert data, each variable characterizes an aspect of one of the possible attack and the property; instructions for formulating a hierarchy in which the plurality of variables are interconnected based on the provided expert data; instructions for determining a state for each of the plurality of variables based on the formulated hierarchy and the provided expert data; instructions for generating a model regarding the possible attack based on the determined states of the plurality of variables and the provided expert data; instructions for assessing risks of the property under the possible attack by the terrorist group based on the generated model; and **instructions for establishing the insurance premium for the property based on the assessed risks**
In regard to claim 10, the same function, risk assessment or analysis, is required to determine the risk to a property and to generate an insurance premium. The risk to a property is a component of determining an insurance premium. Therefore, claim 10 of this application is not patentably distinct from claim 8 of application 10/694,081.		
11. The computer storage medium of claim 10, wherein the instructions for generating the model comprises: instructions for generating a hypothesis regarding the possible attack based on the formulated hierarchy and the provided expert data; instructions for initializing the model based on		9. The computer storage medium of claim 8, wherein the instructions for generating the model comprises: instructions for generating a hypothesis regarding the possible attack based on the formulated hierarchy and the provided expert data; instructions for initializing the model based on

Application 10/694,000		Reference Application: 10/694,081
the generated hypothesis and the provided expert data; and instructions for updating the model based on information outside the generated hypothesis and the provided expert data		the generated hypothesis and the provided expert data; and instructions for updating the model based on information outside the generated hypothesis and the provided expert data.
Claim 11 of this application is not patentably distinct from Claim 9 of application 10/694,081.		
12. The computer storage medium of claim 10, wherein the instructions for determining a state for each of the plurality of variables comprise instructions for determining a linkage between a first variable and a second variable.		10. The computer storage medium of claim 8, wherein the instructions for determining a state for each of the plurality of variables comprise instructions for determining a linkage between a first variable and a second variable.
Claim 12 of this application is not patentably distinct from Claim 10 of application 10/694,081.		
15. The computer storage medium of claim 10, wherein the instructions for providing expert data comprise instructions for providing information regarding a goal of the terrorist group.		11. The computer storage medium of claim 8, wherein the instructions for providing expert data comprise instructions for providing information regarding a goal of the terrorist group.
Claim 15 of this application is not patentably distinct from Claim 11 of application 10/694,081.		
16. The computer storage medium of claim 10, wherein the instructions for providing expert data comprise instructions for providing information regarding an attack delivery method of the terrorist group.		12. The computer storage medium of claim 8, wherein the instructions for providing expert data comprise instructions for providing information regarding an attack delivery method of the terrorist group.
Claim 16 of this application is not patentably distinct from Claim 12 of application 10/694,081.		
17. The computer storage medium of claim 10, wherein the instructions for providing expert data comprise instructions for providing information regarding a weapon likely to be deployed by the terrorist group against the property.		13. The computer storage medium of claim 8, wherein the instructions for providing expert data comprise instructions for providing information regarding a weapon likely to be deployed by the terrorist group against the property.
Claim 17 of this application is not patentably distinct from Claim 13 of application 10/694,081.		
18. The computer storage medium of claim 10, wherein the instructions for providing expert data comprise instructions for providing information regarding a mode of the terrorist group to carry out the possible attack against the property.		14. The computer storage medium of claim 8, wherein the instructions for providing expert data comprise instructions for providing information regarding a mode of the terrorist group to carry out the possible attack against the property.
Claim 18 of this application is not patentably distinct from Claim 14 of application 10/694,081.		
19. A system for **assessing risks of** a property due to terrorist activities, comprising: a database storing expert data, the expert data		15. A system for **establishing an insurance premium usable to insure against risks to** a property due to terrorist activities,

Application 10/694,000		Reference Application: 10/694,081
containing information regarding a possible attack from a terrorist group on the property; an influence determining circuit, routine or application that determines a plurality of variables based on the provided expert data, each variable characterizes an aspect of one of the possible attack and the property; a hierarchy formulating circuit, routine or application that formulates a hierarchy in which the plurality of variables are interconnected based on the provided expert data; a state defining circuit, routine or application that determines a state for each of the plurality of variables based on the formulated hierarchy and the provided expert data; a model creating circuit, routine or application that generates a model regarding the possible attack based on the determined states of the plurality of variables and the provided expert data; an analyzing circuit, routine or application that assesses risks of the property under the possible attack by the terrorist group based on the generated model; and a display generating circuit, routine or application that displays analyzed results.		comprising: a database storing expert data, the expert data containing information regarding a possible attack from a terrorist group on the property; an influence determining circuit, routine or application that determines a plurality of variables based on the provided expert data, each variable characterizes an aspect of one of the possible attack and the property; a hierarchy formulating circuit, routine or application that formulates a hierarchy in which the plurality of variables are interconnected based on the provided expert data; a state defining circuit, routine or application that determines a state for each of the plurality of variables based on the formulated hierarchy and the provided expert data; a model creating circuit, routine or application that generates a model regarding the possible attack based on the determined states of the plurality of variables and the provided expert data; an analyzing circuit, routine or application that establishes the insurance premium for the property under the possible attack by the terrorist group based on the generated model; and a display generating circuit, routine or application that displays analyzed results.
In regard to claim 19, the same function, risk assessment or analysis, is required to determine the risk to a property and to generate an insurance premium. The risk to a property is a component of determining an insurance premium. Therefore, claim 19 of this application is not patentably distinct from claim 15 of application 10/694,081.		
20. The system of claim 19, further comprising: a hypothesis generating circuit, routine or application that generates a hypothesis regarding the possible attack based on the formulated hierarchy and the provided expert data; and a model initializing circuit, routine or application that initializes the model based on the generated		16. The system of claim 15, further comprising: a hypothesis generating circuit, routine or application that generates a hypothesis regarding the possible attack based on the formulated hierarchy and the provided expert data; and a model initializing circuit, routine or application that initializes the model based on the generated

Application 10/694,000		Reference Application: 10/694,081
hypothesis and the provided expert data, wherein the model creating circuit, routine or application updates the model based on information outside the generated hypothesis and the provided expert data.		hypothesis and the provided expert data, wherein the model creating circuit, routine or application updates the model based on information outside the generated hypothesis and the provided expert data.
Claim 20 of this application is not patentably distinct from Claim 16 of application 10/694,081.		
21. The system of claim 19, further comprising: a linkage defining circuit, routine or application that determines a linkage between a first variable and a second variable.		17. The system of claim 15, further comprising: a linkage defining circuit, routine or application that determines a linkage between a first variable and a second variable.
Claim 21 of this application is not patentably distinct from Claim 17 of application 10/694,081.		
24. The system of claim 19, wherein the expert data contains information regarding a goal of the terrorist group.		18. The system of claim 15, wherein the expert data contains information regarding a goal of the terrorist group.
Claim 24 of this application is not patentably distinct from Claim 18 of application 10/694,081.		
25. The system of claim 19, wherein the expert data contains information regarding an attack delivery method of the terrorist group.		19. The system of claim 15, wherein the expert data contains information regarding an attack delivery method of the terrorist group.
Claim 25 of this application is not patentably distinct from Claim 19 of application 10/694,081.		
26. The system of claim 19, wherein the expert data contains information regarding a weapon likely to be deployed by the terrorist group against the property.		20. The system of claim 15, wherein the expert data contains information regarding a weapon likely to be deployed by the terrorist group against the property.
Claim 26 of this application is not patentably distinct from Claim 20 of application 10/694,081.		
27. The system of claim 19, wherein the expert data contains information regarding a mode of the terrorist group to carry out the possible attack against the property.		21. The system of claim 15, wherein the expert data contains information regarding a mode of the terrorist group to carry out the possible attack against the property.
Claim 27 of this application is not patentably distinct from Claim 21 of application 10/694,081.		

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

4. Claims 1 – 3, 6 – 12, 15 – 21, and 24 – 27 are rejected under 35 U.S.C. 102(a) as being anticipated by Risk Management Solutions, Inc (www.rms.com, November, 2002, Terrorism Risk Brochure). Risk Management Solutions, Inc. will be referred to as RMS hereafter.

In regard to claim 1, RMS teaches a method for assessing risks of a property due to terrorist activities, comprising:

- Providing expert data, the expert data containing information regarding a possible attack from a terrorist group on the property (paragraph 3). RMS teaches a model which includes data compiled to determine the probability of a terrorist attack;
- Determining a plurality of variables based on the provided expert data, each variable characterizes an aspect of one of the possible attack and the property (paragraph 3). RMS discloses variables used in the risk assessment of a terrorist attack such as targets (i.e. properties), attack modes, and/or weapons;
- Formulating a hierarchy in which the plurality of variables is interconnected based on the provided expert data (paragraphs 55 – 58). RMS discloses a tier

system in which the variables (i.e. target) are ranked according to the appeal of the target to a terrorist;

- Determining a state for each of the plurality of variables based on the formulated hierarchy and the provided expert data (paragraph 64), where for examining purposes the Examiner has interpreted "state" to refer to the status of the variables. RMS teaches a system in which cities are ranked according to their attractiveness (using variables such as location, industry, etc.) to a terrorist group.
- Generating a model regarding the possible attack based on the determined states of the plurality of variables and the provided expert data (paragraph 69); and
- Assessing risks of the property under the possible attack by the terrorist group based on the generated model (paragraph 69).

In regard to claim 2, RMS teaches the method according to claim 1, wherein generating the model comprises:

- Generating a hypothesis regarding the possible attack based on the formulated hierarchy and the provided expert data (paragraph 79);
- Initializing the model based on the generated hypothesis and the provided expert data (paragraphs 69, 79, and 80); and

- Updating the model based on information outside the generated hypothesis and the provided expert data (paragraph 87); RMS discloses that the risk assessment model is updated as needed.

In regard to claim 3, RMS teaches the method according to claim 1, wherein determining a state for each of the plurality of variables comprises determining a linkage between a first variable and a second variable (paragraph 79) where RMS discloses a model of attack types liked to contributing factors (i.e. time, weather).

In regard to claim 6, RMS teaches the method according to claim 1, wherein providing expert data comprises providing information regarding a goal of the terrorist group (paragraph 12).

In regard to claim 7, RMS teaches the method according to claim 1, wherein providing expert data comprises providing information regarding an attack delivery method of the terrorist group (paragraph 3).

In regard to claim 8, RMS teaches the method according to claim 1, wherein providing expert data comprises providing information regarding a weapon likely to be deployed by the terrorist group against the property (paragraph 19).

In regard to claim 9, RMS teaches the method according to claim 1, wherein providing expert data comprises providing information regarding a mode of the terrorist group to carry out the possible attack against the property (paragraph 3).

In regard to claim 10, RMS teaches a computer storage medium having executable software code for assessing risks of a property due to terrorist activities, the executable soft-ware code including:

- Instructions for providing expert data, the expert data containing information regarding a possible attack from a terrorist group on the property (paragraphs 3 and 82);
- Instructions for determining a plurality of variables based on the provided expert data, each variable characterizes an aspect of one of the possible attack and the property where the selected attack scenarios are considered variables (paragraphs 3, 82, and 84);
- Instructions for formulating a hierarchy in which the plurality of variables are interconnected based on the provided expert data (paragraphs 55 – 58, 81 and 82);
- Instructions for determining a state for each of the plurality of variables based on the formulated hierarchy and the provided expert data (paragraphs 20 and 82);

- Instructions for generating a model regarding the possible attack based on the determined states of the plurality of variables and the provided expert data (paragraphs 69 and 82); and
- Instructions for assessing risks of the property under the possible attack by the terrorist group based on the generated model (paragraphs 69 and 82).

In regard to claim 11, RMS teaches the computer storage medium of claim 10, wherein the instructions for generating the model comprise:

- Instructions for generating a hypothesis regarding the possible attack based on the formulated hierarchy and the provided expert data (paragraph 79);
- Instructions for initializing the model based on the generated hypothesis and the provided expert data (paragraphs 69, 79, and 80); and
- Instructions for updating the model based on information outside the generated hypothesis and the provided expert data (paragraph 87).

In regard to claim 12, RMS teaches the computer storage medium of claim 10, wherein the instructions for determining a state for each of the plurality of variables comprise instructions for determining a linkage between a first variable and a second variable (paragraph 79), where RMS discloses a model of attack types linked to contributing factors (i.e. time, weather).

In regard to claim 15, RMS teaches the computer storage medium of claim 10, wherein the instructions for providing expert data comprise instructions for providing information regarding a goal of the terrorist group (paragraph 12).

In regard to claim 16, RMS teaches the computer storage medium of claim 10, wherein the instructions for providing expert data comprise instructions for providing information regarding an attack delivery method of the terrorist group (paragraph 3).

In regard to claim 17, RMS teaches the computer storage medium of claim 10, wherein the instructions for providing expert data comprise instructions for providing information regarding a weapon likely to be deployed by the terrorist group against the property (paragraph 19).

In regard to claim 18, RMS teaches the computer storage medium of claim 10, wherein the instructions for providing expert data comprise instructions for providing information regarding a mode of the terrorist group to carry out the possible attack against the property (paragraph 3).

In regard to claim 19, RMS teaches a system for assessing risks of a property due to terrorist activities, comprising:

- A database storing expert data, the expert data containing information regarding a possible attack from a terrorist group on the property (paragraphs 2, 5, and 62);

- An influence determining circuit, routine or application that determines a plurality of variables based on the provided expert data, each variable characterizes an aspect of one of the possible attack and the property (paragraphs 5 - 7);
- A hierarchy formulating circuit, routine or application that formulates a hierarchy in which the plurality of variables are interconnected based on the provided expert data (paragraphs 55 – 58 and 62);
- A state defining circuit, routine or application that determines a state for each of the plurality of variables based on the formulated hierarchy and the provided expert data (paragraphs 5 – 9 and 62);
- A model creating circuit, routine or application that generates a model regarding the possible attack based on the determined states of the plurality of variables and the provided expert data (paragraphs 9 and 69);
- An analyzing circuit, routine or application that assesses risks of the property under the possible attack by the terrorist group based on the generated model (paragraph 80); and
- A display generating circuit, routine or application that displays analyzed results (page 14). Figure A illustrates a screen shot of a risk analysis/assessment model of property loss/workers compensation due to a possible terrorist attack.

In regard to claim 20, RMS teaches the system of claim 19, further comprising:

- A hypothesis generating circuit, routine or application that generates a hypothesis regarding the possible attack based on the formulated hierarchy and the provided expert data (paragraph 79); and
- A model initializing circuit, routine or application that initializes the model based on the generated hypothesis and the provided expert data (paragraphs 69, 79, and 80); and,
- Wherein the model creating circuit, routine or application updates the model based on information outside the generated hypothesis and the provided expert data (paragraph 87).

In regard to claim 21, RMS teaches the system of claim 19, further comprising: a linkage defining circuit, routine or application that determines a linkage between a first variable and a second variable (paragraph 79).

In regard to claim 24, RMS teaches the system of claim 19, wherein the expert data contains information regarding a goal of the terrorist group (paragraph 12).

In regard to claim 25, RMS teaches the system of claim 19, wherein the expert data contains information regarding an attack delivery method of the terrorist group (paragraph 3).

In regard to claim 26, RMS teaches the system of claim 19, wherein the expert data contains information regarding a weapon likely to be deployed by the terrorist group against the property (paragraph 19).

In regard to claim 27, RMS teaches the system of claim 19, wherein the expert data contains information regarding a mode of the terrorist group to carry out the possible attack against the property (paragraph 3).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 4, 13, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over RMS in view of Fricker Jr. et al. (Fricker, Jr. et al. Rand Corporation. Issue Paper: Measuring and Evaluating Local Preparedness for a Chemical or Biological Attack. 2002).

In regard to claim 4, RMS teaches a method, as per claim 1, for assessing risks of a property due to terrorist activities.

RMS fails to teach a method further comprising establishing training programs for responding to the attack based on the assessed risks.

Fricker, Jr. teaches a method further comprising establishing training programs for responding to the attack based on the assessed risks (page 4, paragraph 16). Fricker et al. Jr. discloses training using live and/or tabletop exercises.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include a method further comprising establishing training programs for responding to the attack based on the assessed risks as taught by Fricker, Jr. et al. with the motivation of ensuring the public sector is prepared to respond to terrorist attack by a variety of methods (page 1, paragraph 3).

In regard to claim 13, RMS teaches a computer storage medium having executable software code for assessing risks of a property due to terrorist activities, as per claim 10.

RMS fails to teach the computer storage medium further comprising: instructions for establishing training programs for responding to the attack based on the assessed risks.

Fricker Jr. et al. teaches a computer storage medium further comprising: instructions for establishing training programs for responding to the attack based on the assessed risks (page 4, paragraph 16).

The motivation to combine the teachings of RMS and Fricker Jr. is discussed in the rejection of claim 4, and incorporated herein.

In regard to claim 22, RMS teaches a system for assessing risks of a property due to terrorist activities, as per claim 19.

RMS fails to teach a system wherein the analyzing circuit, routine or application establishes training programs for responding to the attack based on the assessed risks.

Fricker Jr. et al. teaches a system wherein the analyzing circuit, routine or application establishes training programs for responding to the attack based on the assessed risks (page 4, paragraph 16).

The motivation to combine the teachings of RMS and Fricker Jr. et al. is discussed in the rejection of claim 4, and incorporated herein.

7. Claim5, 14, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over RMS in view of Kumar et al. (U.S. Patent No. 7,308,388 B2).

In regard to claim 5, RMS teaches a method, as per claim 1, for assessing risks of a property due to terrorist activities.

RMS fails to teach a method further comprising: providing information for selecting a vacation or retirement site based on the assessed risks.

Kumar et al. teaches a method further comprising: providing information for selecting a vacation or retirement site based on the assessed risks (paragraph [0235]). Kumar et al. discloses a method in which predefined high risk zones are utilized for risk assessment. This information can be utilized for terrorist activities, thus, a person seeking a vacation or retirement site can utilize the information taught by Kumar et al. and apply it to their search for a site. Although Kumar et al. does not specifically teach

a vacation or retirement site, it is obvious that the invention by Kumar et al. can be utilized to determine a suitable vacation or retirement site base on the risk assessment.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include a method further comprising providing information for selecting a vacation or retirement site based on the assessed risks as taught by Kumar et al. with the motivation of enabling a user or customer the ability to select a site based on its relative safety by using a risk assessment tool (paragraph [0017]).

In regard to claim 14, RMS teaches a computer storage medium having executable software code for assessing risks of a property due to terrorist activities, as per claim 10.

RMS fails to teach a computer storage medium further comprising: instructions for providing information for selecting a vacation or retirement site based on the assessed risks.

Kumar Jr. et al. teaches a computer storage medium further comprising: instructions for providing information for selecting a vacation or retirement site based on the assessed risks (paragraph [0235]).

The motivation to combine the teachings of RMS and Kumar is discussed in the rejection of claim 5, and incorporated herein.

In regard to claim 23, RMS teaches a system for assessing risks of a property due to terrorist activities, as per claim 19.

RMS fails to teach a system wherein the analyzing circuit, routine or application provides information for selecting a vacation or retirement site based on the assessed risks.

Kumar et al. teaches a system wherein the analyzing circuit, routine or application provides information for selecting a vacation or retirement site based on the assessed risks (paragraph [0235]).

The motivation to combine the teachings of RMS and Kumar et al. is discussed in the rejection of claim 5, and incorporated herein.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Sandia National Laboratories News Release. July 19, 2001. Tool Against Terrorism and other Disasters: Sandia to Release First Risk-Based Approach to Building Management Software for Use by GSA.
- "Software Analyzes Potential Threats to Buildings." Madonna Aveni. Civil Engineering. New York: Oct 2001. Vol. 71, Iss. 10, p. 36.

- U.S. Patent Application Publication 2005/0043961 A1 (Torres et al.) discloses a software system which, using real-time and historical data, detects fraud and terrorist activities/behavior.
- U.S. Patent No. 7,308,388 B2 (Beverina et al.) discloses a method and apparatus for risk management. The risk management tool includes a database containing information about individuals, groups, locations, historical events, and other information. The invention calculates the risk of an undesirable event.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KRISTINE K. RAPILLO whose telephone number is (571)270-3325. The examiner can normally be reached on Monday to Thursday 6:30 am to 4 pm Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Thomas can be reached on 571-272-3776. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KKR

JOSEPH THOMAS
SUPERVISORY PATENT EXAMINER